## AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph on page 2, lines 17-26 with the following amended paragraph:

Preferred ~~embodiment~~ embodiments of the present invention can also be viewed as providing methods for the automated diagnosis of security and reliability problems for electronic profile or policy enabled systems. In this regard, one embodiment of such a method, among others, can be broadly summarized by the following steps: identifying recent configuration changes made to the electronic system that fall within pre-established parameters; ranking the identified changes into potential causes; verifying ranked potential causes to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and calculating distances associated with the ranked potential causes to help determine the actual likelihood that one or more of them are the true cause.

Please replace the paragraph on page 4, lines 5-19 with the following amended paragraph:

Referring now in more detail to the drawings, in which like numerals indicate corresponding parts throughout the several views, FIG. 1 is a block diagram depicting a preferred embodiment of a system 100 for automated diagnosis of security and reliability problems for electronic profile or policy enabled systems. By way of explanation, policy refers to system configuration information. Changing the operation of the system (or a part of the system) involves modifying policy or profile information. Profiles are used to divide entities into different groups or categories to reduce the information and effort needed to manage ~~management~~ the network or system. For example, in a network, routers might be divided into edge, intermediate and core routers (i.e., three router profiles). Each profile has a different policy definition defining membership. Within the policy for that network, different rules and configuration is delineated for each group. Thus, if a particular router is a core router, a portion of its default configuration is defined as part of a "core router" configuration and is identical to

other core router, thus reducing the amount of policy information needed for the profile of core routers.

Please replace the paragraph on page 7, line 19 through page 8, line 2 with the following amended paragraph:

FIG. 2 is a block diagram depicting a more detailed illustrative example of a preferred embodiment of a system 200 for providing automated diagnosis of security and reliability problems for electronic profile or policy enabled systems. The system 200 includes the computing device 108 that communicates with the user processing device 102, provider network 104, and databases 112, 114 configured as an index database (EDD) 210 and a hierarchical vulnerability database (HVD) 212. The computing device 108 further includes memory 122 having operating system 128 and logic 130 configured as a central diagnosis engine 206, presentation module 204 and database interface module 208. Further, computing device 108 includes local interface 124, processor [[122]] 120, network interface card 214 and system interfaces 126, 126A. In an example, the user processing device 102 communicates with the computing device 108 via the I/O 126A. In another preferred embodiment, the user processing device 102 communicates with the computing device 108 via the provider network 104. In a preferred embodiment, the network interface card 214, I/O 126, and database interface modules 208 are utilized for communicating between the provider network 104 and the databases 210, 212.

Please replace the paragraph on page 9, lines 14-25 with the following amended paragraph:

FIG. 3 is a block diagram of an illustrative example of a preferred embodiment of modules of a ~~sequential examination~~ central diagnosis engine 206 of a system for automated diagnosis of security and reliability problems for electronic profile or policy enabled systems. In a preferred embodiment, the central diagnosis engine 206 includes a possible cause accumulator module 302 that couples to the presentation module 204, distance estimator module 304, verifier

module 306, and rank estimator module 308, a problem accumulator module 310 that couples to an input parser/filter module 312 and a cause estimator module 314, and a policy interpreter module 316 that couples to the verifier module 306 (and optionally to a policy-management system 320 via the network 104). The verifier module 306 is also coupled to the database interface module 208. An adaptive logger 318 couples to a policy-based management system 320 either directly or via the provider network 104.

Please replace the paragraph on page 9, line 26 through page 10, line 14 with the following amended paragraph:

The input parser/filter module 312 receives security or reliability problem description input from a user's processing device 102 (or an administrator) in a plurality of formats, such as data files of an acceptable format, or other input either automatically provided by monitoring, sensor or management, or manually in response to prompting from the presentation module 204, among others. In one preferred embodiment, the input parser/filter module 312 utilizes standard software engineering techniques to convert the input data into data usable by the problem accumulator module [[312]] 310. The input parser/filter module 312 preferably interacts with the user's processing device 102 via application programming interfaces that are consistent with the user's operating system, for instance, Unix, Linux, windows, etc., with the details of the interfaces being dependent upon the specific implementation including the choice of software language and design. In a preferred embodiment, the implementation is selected to perform the specific conversions needed for each allowed input type. During the conversion process, the input parser/filter module 312 filters out extraneous data, such that only pertinent input remains. In an alternative embodiment, sensor and/or monitoring systems 322 from which the input parser/filter module 312 could receive security problem data includes, firewalls, security or reliability related sensors, other monitoring sensors, other monitoring devices, and intrusion detection systems (collectively referred to as IDS). IDSs in particular are typically designed to provide alarms and alerts, with associated electronic messages, when detecting security problems or attacks in progress and thus are suitable inputs to the input parser/filter module 312.

Please replace the paragraph on page 10, lines 15-21 with the following amended paragraph:

In a preferred embodiment, the problem accumulator module [[304]] 310 receives problem descriptive data from the input parser/filter module 312 and cycles, continuing to receive data until the problem is fully described. The problem can be fully described, for instance, by a user finishing inputting data or the completion of the automatic transfer of information from a sensor or monitoring 322. In a preferred embodiment, the problem accumulator module [[304]] 310 provides the completed set of problem descriptive data to the cause estimator module 314.

Please replace the paragraph on page 11, lines 19-28, with the following amended paragraph:

The adaptive logger 318 also interfaces with the cause estimator module 314. In an example, the adaptive logger 318 records, for ~~example~~ example, log policy changes that occur, thus being termed a "logger." The adaptive logger 318 may adjust its recording in an adaptive manner by for example, modifying the focus or granularity, i.e., level of detail, in response to problem encountered. As an example, if security or reliability problems are encountered with router interface configuration, the adaptive logger 318 records greater detail than normally recorded in response to noting these problems. This provides for more effectively dealing with similar problems in the future. In a preferred embodiment, after a configurable time period, such as a week or month, the recording granularity of the adaptive logger 318 could revert to its normal setting.

Please replace the paragraph on page 13, lines 11-25, with the following amended paragraph:

Regarding whether the problem occurred on the same piece of equipment as the policy change, the ranking process performed by the rank estimator module 308 determines if the policy change and problem are co-located, and if [[so]] so, assigns a difference of zero (otherwise a large difference is assigned, e.g. 50). Regarding different types of equipment, type values are

used with an assumed problem parameter value of 100. For example, if the policy change occurs on an element that is highly security sensitive, for example a firewall or intrusion detection system, a high type value is assigned (e.g., 75). A less security sensitive element, for example a router or Ethernet switch, is assigned a low value (e.g., 10). For equipment between these two levels of security, for instance, a server, an intermediate type value is assigned (e.g., 40). Type values can be assigned for all types of equipment and sub-equipment that reflect established security knowledge and expertise. Similar values can be assigned for reliability components. In an example, for each policy change (or potential cause) the actual parameter difference is the assumed problem parameter value of 100 minus the associated type value.